

2008

Power and Practice in Information Systems Security Research

Mikko Siponen

University of Oulu, msiponen@tols16.oulu.fi

Robert Willison

Copenhagen Business School, rw.inf@cbs.dk

Richard Baskerville

Georgia State University, baskerville@acm.org

Follow this and additional works at: <http://aisel.aisnet.org/icis2008>

Recommended Citation

Siponen, Mikko; Willison, Robert; and Baskerville, Richard, "Power and Practice in Information Systems Security Research" (2008).
ICIS 2008 Proceedings. 26.

<http://aisel.aisnet.org/icis2008/26>

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

POWER AND PRACTICE IN INFORMATION SYSTEMS SECURITY RESEARCH

Pouvoir et pratique dans la recherche sur la sécurité des systèmes d'information

Completed Research Paper

Mikko Siponen

Dept. of Information Processing Science,
University of Oulu,
Linnanmaa,
P.O. Box 3000,
FIN 90014,
Oulun yliopisto,
Finland
msiponen@tols16.oulu.fi

Robert Willison

Department of Informatics,
Copenhagen Business School,
Howitzvej 60,
DK – 2000 Frederiksberg
Copenhagen,
Denmark,
rw.inf@cbs.dk

Richard Baskerville

Department of Computer Information Systems
Georgia State University,
P.O. Box 4015,
Atlanta,
Georgia 30302-4015
USA
baskerville@acm.org

Abstract

This paper examines the domination of information systems security research by a non-intellectualist tradition. Based on an in-depth examination of the published research literature in this area, we show how a symbolic system of practical logic prevails across this field. We compare the symbolic systems present in the information systems security research literature and that of the general information systems research literature. This comparison demonstrates that research practices in information systems security are, in key ways, opposite to the research practices in the general field of information systems. An understanding of these cultural values helps to recognize avenues to improve future research practices in the information systems security field, with implications for improving research practices in the information systems field as a whole.

Keywords: Information Systems Security, Information Systems Research, Social Capital, Cultural Capital, Symbolic Capital

Résumé

Cette recherche montre comment un système symbolique de la logique pratique domine la recherche sur la sécurité des systèmes d'information. Les pratiques dans le domaine de la sécurité des systèmes d'information, en matière de recherche, sont opposées au champ général des systèmes d'information.

1. Introduction

In recent years organizations have paid increasing attention to information systems security (ISsec). This is understandable given the sheer amount of information now in digital form. The desire to secure such information has been fuelled by concerns over the rising number of corporate security breaches (Dhillon and Backhouse, 2001). One security survey, for example, noted how in 1997, 37% of respondents reported a breach (Thompson, 1998). However, more recent surveys have reported a figure averaging 90% (Bagchi and Udo 2003, p. 684; Hinde 2002, p. 310).

This need for effective information systems (IS) security should drive strong academic activity in fields like computer science, computer engineering, and information systems. However, anecdotal evidence published along with existing ISsec survey research suggests that the specific research in ISsec lags behind the general advances in IS. For example, Baskerville (1992) details a discord between systems development methods in general and security development methods in particular. This discord arises because security methodologies are underdeveloped, and security work lags behind general IS research. These results are conformed by a recent study (Siponen, 2005).

These anecdotal references to a general deficiency in ISsec research arise tangentially in the context of literature surveys that intend other purposes. In this paper, we explore whether such deficiencies exist indeed, and why these deficiencies persist. We examine the first part of this question through an extensive literature review. In this review we analyze three main ISsec journals and the top twenty IS journals for the period 1990-2004. In total 1280 ISsec papers are assessed. We explore the second part of this question through an analysis informed by Pierre Bourdieu's theory of practice. In this analysis, we compare the newly revealed features of the ISsec research literature with the known features of the more general IS research literature.

2. Explanatory Framework

The explanatory part of this study examines social domination and social reproduction in professional settings where scholarly and practical values compete. Academic disciplines operate as a society that lacks a judicial apparatus, a formal government, a self-regulating market, etc. Domination occurs through the reproduction of capital structures. However, in the academic case, it is not economic capital, but social and symbolic capital (Bourdieu 1977, pp. 183-184).

Once we delineate how the ISsec research literature has been shaped in a distinctively different way than the general IS research literature, we will need these concepts in order to understand how these features have evolved and continue to reproduce. This social reproduction is related to our professional habits. We all have individual and shared professional habits, but we use the term *habitus* in a deeper sense than just our professional habits. It is a socialized, habitual way in which professionals think about their practice. The *habitus* embodies the active presence of our forgotten professional history and it gives practices themselves certain autonomy. *Habitus* can function as a form of accumulated capital (Bourdieu, 1990, p. 56). *Habitus* is a complex weld of unconscious, objective social structures and subjective behavior of practice, as if social beings are the unknowing agents of their own social histories. *Habitus* can be individual or shared depending on how we wish to delineate a particular *habitus*.

We use the term *field* to describe a social space in which social beings engage each other in their various struggles with means for ends. The *habitus* is a socialized body that incorporates the structures of the field thus defining perceptions of, and actions within, the field. (Bourdieu 1998, p. 32)

There are various kinds of capital that operate according to the values structured within the *habitus* and the field. These include economic capital, cultural capital, political capital, and symbolic capital. Cultural capital is related to mind and thought, the realm of artists, authors, and professors. It is often embodied by class distinctions and societies (Bourdieu 1998, pp. 4-5). Political capital guarantees its holders a form of private appropriation of goods

and public services such as homes, cars, hospitals, schools, etc. (Bourdieu 1998, p. 16). Symbolic capital is an ordinary property like strength, wealth, wisdom, courage, which habitus endows with importance and power (Bourdieu 1998, p. 102). Symbolic capital includes the qualities that construct a strong professional reputation, and has deep value to professionals in their practice. Habitus can define and transform economic, cultural, and political capital into symbolic capital.

From a perspective centered on information systems, we might assume, based on naming alone, that “information systems security” is necessarily subsumed as some form of sub-discipline under “information systems”. Yet the discord between IS and IS sec leads us to question this assumption. Does this assumption hold under close scrutiny? In this paper we will analyze and delineate the distinctive differences between the IS and ISsec research literatures. With the distinctions clarified, we are able to explain the continuing distinctions (and the discord) by applying Bourdieu’s concepts, particularly the differences in symbolic capital between the IS habitus and the ISsec habitus. If ISsec is indeed a sub-discipline of IS, the habitus should largely overlap. If the habitus of each is not shared with the other, the assumption that ISsec is a sub-discipline of IS does not hold.

We use Bourdieu’s concepts to analyze the differences between the symbolic capital valued in the habitus of the two disciplines. While Bourdieu’s framework apply broadly across many fields of practice, we must find more immediately relevant frameworks to reveal the symbolic capital important in information systems in a way that can be compared with those of ISsec. Other frameworks (e.g. Laudon, see below) are available that help uncover the symbolic capital (although these do not use Bourdieu’s labels) in the discipline of IS. Through such “applied” frameworks we find the values in IS that enable us to analyze its similarities and differences with ISsec using Bourdieu’s theories of habitus and symbolic capital.

2.1 Framing Research Literature Features

In order to enable a comparison between the ISsec research literature and more general IS research literature, a common conceptual framework is required. For this purpose, we considered different frameworks that have been used by IS scholars. Hirschheim et. al. (1995, 1996) and Iivari et. al. (2001) used Burrell and Morgan’s sociological paradigms to review methods for IS development. Iivari et. al. (1998) have analyzed IS development methods in the terms of research methods, the organizational role of IS, and research objectives. Kuhn’s work on paradigms has influenced Iivari’s (1991) research, while Farhoomand (1987) applies Popper’s view of science.

While these philosophical views have produced interesting findings, there are deficiencies. Both Burrell and Morgan (1979) and Kuhn (1970) take a relativist position with regard to ‘paradigms’. This means that different paradigms are incommensurable by definition. If we follow the views of Burrell and Morgan (1979) and Kuhn (1970) to the letter, then a perspective anchored in one paradigm, say a “positivist”, cannot correctly interpret nor criticize research within other paradigms, say “interpretivist”. For Kuhn, the incommensurability occurs as a result of the fact that different paradigms define their own fundamental assumptions regarding research methods, validation, and even language. Since different scholars operated within different paradigms “practice their trades in different worlds”, their findings are not comparable in any way across different paradigms. As a consequence, because scientific revolutions represent an “all-or-nothing” form of change, there is no progress in science, according to Kuhn (1970, p. 150)¹. Similarly, Burrell and Morgan (1979) argue that research within different paradigms is not comparable, and hence meaningful conversations between different paradigms are not possible. In addition they insist that different paradigms must not be reconciled.

Chua (1986), Iivari (1991) and Landry and Banville (1992) argue that such incommensurable views – (1. impossible to measure and compare research across paradigms; 2. any discussions across paradigms are meaningless, 3. paradigms should not be integrated) – are unnecessarily regarded as limits to the scientific discourse. If inter-paradigmatic research is incommensurable, research within a paradigm would be immune to external criticism. This then leads to the position where research quality would be difficult to measure, since everything would be accepted simply by appealing to the incommensurability of a paradigm. One practical solution is offered by Laudan (1984), who advances a reticulated model of science (see also Landry and Banville, 1992). Since this model seeks to operate across paradigms, we use it as a framework for the common features of ISsec research literature that promises comparability with the more general IS research literature.

¹ Kuhn sees that scientific revolutions are “non-cumulative developmental episodes in which an older paradigm is replaced in whole or in part by an incompatible new one.” (Kuhn, 1970 p. 92).

2.2 Laudan's framework

Laudan (1984) proposes the Reticulated Model of Science which consists of theories, methods, and aims (goals, ends, values). In his view, changes in theories, methods, and aims are piecemeal and happen one at a time, rather than the all-or-nothing position as proposed by Kuhn². In addition, aims, methods and theories are rationally negotiable. In opposition to Kuhn (1970), conceptual dialogue across paradigms is a potential source of progress in science (Batts and Crawford 1991, p. 348). For Laudan (1984), there is no one aim (e.g., "truth") in science. Finally, science is progressive, since scientific progress is nothing more than progress towards our goals. If the goal changes, then the criterion regarding what constitutes progress changes. Therefore, progress in science, though relative to fixed goals, can be rationally evaluated.

In summary, there are three elements of Laudan's Reticulated Model of Science: Theories, methods and aims. Next we describe how we use these elements in our analysis, and also point out their importance in the IS literature.

2.3 Theories and research methods

As discussed below, the application of theory and the use of appropriate research methods are seen as essential and elementary features of any research (Truex et. al. 2006). In the IS field, this view is also shared by natural science (often referred to as positivists) and social science orientated (often referred to as interpretivists) scholars (Culnan, 1987; Landry and Banville, 1992). The importance of theory and research methods, is further recognized by supporters of "IS-as-a-design-science" view, which asserts that IS research does not easily fit into the models of the social or natural sciences (Walls et. al. 1992, Walls et. al. 2004). In fact, Gregor (2006) distinguishes five types of theories used in the IS field. Our use of theories includes all of these types of theories.

However, the use of theory requires in-depth expertise in the discipline to which the theory belongs (Truex et. al. 2006; Walsham, 1997). In an attempt to assess the quality of the theories applied in IS security, and the manner in which they are used, we refer back to Laudan's (1984) "reticulated model of science". Laudan argues that a theory must be in accordance with the research method used and the goals of the research, which, interestingly, is also suggested by Truex et. al. (2006 pp. 809-812). To adapt a simple interpretation of this view: a theory has to be used so that it contributes something to the study/topic that would most likely be lacking in its absence (Truex et. al. 2006, p. 812)³. That is, studies only referring to theory as skin deep do not meet this criterion. To illustrate such a use of a theory, in their article on the use of design theory, Walls et. al. (2004, p. 55) describe four levels. At the first level, design theory is referred to at a superficial level, as a "cloak of theoretical legitimacy", without indicating how exactly the design theory guides the research. In our analysis, we would not classify such studies as based on design theory.

The research method classification was adopted from Galliers (1992), which includes: laboratory experiment, field experiments, surveys, theorem proof, subjective/argumentative, case studies, forecasting and future research, simulation and, finally, action research. 'Laboratory experiments' refer to tests carried out in such an environment, while 'field experiments' utilize natural science methods to study phenomena in the field rather than in the context of a laboratory. While 'surveys' are used to collect quantitative information (Straub, 1989), 'case studies' focus on in-depth studies of a single event, hence the name, 'case' (Yin, 2002). 'Theorem proof' refers to non-empirical research containing theorems and their proofs, typically used in the field of Computer Science (Lending et. al. 1992, p. 5). 'Subjective/argumentative' refers to conceptual-theoretical research. 'Simulation' refers to quantitative modeling of systems in order to understand their functioning. 'Action research' takes a similar form to case studies, with a notable difference being the iterative action research cycle (Baskerville and Wood-Harper, 1998).

² Kuhn sees that theories, methods and aims in science form an inseparable package: scholars cannot modify one without modifying the others (Laudan 1984).

³ Truex et. al. (2006 p. 812) note that "What is added value to the theorizing process when using theory x that is not added when using theory y?". While their idea does not come from Laudan (1984), it is, however, in synchronization with Laudan's "reticulated model of science".

We also added a research method called 'secondary data' to Gallier's classification (1992). During the analysis the authors identified papers, which used such data as a basis for their methodology, hence it was decided that the category should be created.

2.4 Research topics (aims)

Within IS, the examination of the research topics, which constitute a specific field is considered to be highly relevant. Such examination helps to throw light on the type of research, and ultimately the very nature of the subject area itself (Bacon and Fitzgerald, 2001). There are two ways of forming a research topic classification. One method is to "let the published works speak themselves", i.e., analyze the literature while avoiding the use of a predefined classification systems (Bacon and Fitzgerald, 2001). In other words, produce a classification based on a theory creating or 'grounded theory' type of method. An alternative approach is to use a priori theory or classification systems such as the ISRL categories or the ACM classification system (as used by Vessey et. al. 2002). The former method was chosen for the purpose of this study for the following reasons. First, the authors wanted to offer a genuine and comprehensive picture of IS security research. It can be argued that existing classification schemas (for example the ACM categorization), reflect a limited computer science perception of security research. Furthermore, a classification of the literature, "starting with a clean slate", offers the potential for an updated view of the field, as opposed to the use of a predefined classification system. In addition, when using predefined classification systems, like the ACM, no insight is offered into how such typologies are created. Predefined classifications may also not reflect the actual research in the field. For instance, Zhang and Li (2005, p. 272) noted this difficulty when using predefined classification schema for analyzing HCI research. In fact, using a strategy based on 'let the published works speak for themselves', may even contribute to such classification schemas as advanced by the ACM.

3. Features of Information Systems Security Research Literature

3.1 Existing ISsec Research Literature Surveys

Previous literature reviews in IS security have focused on the methods for the development of secure systems (Baskerville 1992; Siponen 2005a,b; Villarroel et. al. 2005). In addition, the IS security literature has been analyzed using sociological paradigms by Burrell and Morgan to illustrate the need for understanding the social as well as technical aspects of the control environment (Dhillon and Backhouse, 2000) – see Table 1.

Table 1. Existing IS Security Literature Reviews		
Article	Area	Number of articles analyzed
Baskerville (1993)	Methods for the development of secure systems.	19
Dhillon and Backhouse (2001)	IS security literature.	11
Siponen (2005a)	Methods for the development of secure systems.	17
Siponen (2005b)	Methods for security management and the development of secure systems.	17
Villarroel, Fernandez-Medina and Piattini (2005)	Methods for the development of secure systems.	11

While there is no doubt that these studies have provided a number of important insights for IS security research and practice, they have certain limitations. First, the number of IS security articles covered by these studies are relatively small (Table 1). Second, none of these studies apply inter-rater reliability criteria. The latter refers to a method whereby the literature is reviewed separately by two or more individuals, known as coders or raters. In this study, two coders were used. To the best of our knowledge, this is the first attempt to review the literature in this manner.

3.2 Literature analysis methodology

In order to compare the ISsec literature with the IS literature, we must create this survey from the whole cloth. To classify research within a specific IS field, scholars have analyzed key words, abstracts or full texts (Vessey et. al. 2002). This study is based on the analysis of full texts, as it was considered the most reliable method of reviewing the literature and developing a research topic classification (see Siponen and Willison (2007) for further details).

To increase the reliability of the analysis, we applied the inter-rater reliability criteria as follows. The first stage of analysis involved the authors separately reviewing the relevant literature, and identifying tentative categories of classification. The authors then critically discussed their initial analyses and through this process reached a consensus with regard to the most suitable forms of classification.

3.3 Literature analysis scope

The scope of the literature survey covered three ISsec journals and the top 20 IS journals. The ISsec journals included Computers & Security, Information Management & Computer Security and Information Systems Security. These were chosen as they act as the three major publications in the field. Other publications including the Journal of Computer Security and ACM Transactions on Information and Systems Security were omitted from the research. These well known security forums were classified as computer science forums based on their editorial policy and the type of papers published in them. In addition, the top 20 IS journals were analyzed. There are well known ranking lists, the most notable being the combination of six ranking studies (see <http://www.isworld.org/csaunders/rankings.htm>). This list, however, includes journals within related disciplines that do not really contain IS papers (Chua et. al. 2002), not to mention IS security papers. As a consequence, the list may not fully reflect the status of the journals in the field. For example, JAIS is often, (as per the Saunders ranking), ranked below CAIS (Lyytinen in JAIS editorial on 2006). For these reasons, we selected a list that primarily ranks IS journals (Peffer and Tang, 2003). The IS journals in the list are: CAIS, JACM, ISF, IT&P, EJIS, ISR, JSIS, ISJ, JCIS, IRMJ, I&M, JMIS, JAIS, MISQ, JofDM, DSS, JGinfMgt and IJofECom.

The period of analysis covers 15 years (from 1990 to 2004) and compares well with similar IS research projects. Indeed, Zhang and Li (2005), whose review of the HCI literatures covers 13 years note how their study 'is more than double the period that is normally used in this type of research'. As a consequence we feel that our period of analysis is more than justified. The number of IS security papers analyzed amounted to 1280. Once again, this figure can be viewed in a favorable light when compared with similar IS research (Culnan 1987; Zhang and Li 2005; Iivari et. al. 2004).

3.4 Theories Used In IS Security Research

In total 38 theories were identified through our analysis. Of the 1280 papers we analyzed, 237 (18.51%) included one or more of these theories. By far the largest category identified was 'mathematics' accounting for 189 papers, which represents nearly 80% (79.74%) of all the articles containing theory. Hence the other 37 theories accounted for just over twenty percent of the remaining (48) papers. This means that 30 of the 37 theories were cited once. The remaining seven theories included six which were cited twice, leaving General Deterrence Theory which was referenced in six papers.

3.5 Methods Used In IS Security research

With regard to the research methods used in the articles, the 'subjective-argumentative' category, accounted for 996 (77.81%) papers. The remaining nine categories, therefore, covered the other 284 papers. Of this total, 146 (11.40%)

were categorized as ‘theorem proof’ texts. If we combine the ‘subjective-argumentative’ and ‘theorem proof’ total, the figure comes to 1,142 (89.21%) papers. Hence, the remaining categories (field experiment, survey, action research, case research, forecast, simulation, laboratory experiments and secondary data) accounted for 138 (10.79%) papers.

3.6 Topics in IS security research

Our analysis identified fifty-nine research topics. Despite this large number, 14 categories constitute 71.95% of all the papers. These categories (with over 30 papers or more) include ‘legal aspects of IS security’ (43 = 3.35%), ‘general IS security’ (85 = 6.64%), ‘business continuity planning’ (41 = 3.20%), ‘IS security management and planning’ (113 = 8.82%), ‘OS security’ (32 = 2.50%), ‘risk management’ (38 = 2.96%), ‘viruses and malware’ (61 = 4.76%), ‘computer-crime’ (32 = 2.50%), ‘database security’ (80 = 6.25%), ‘intrusion detection systems’ (38 = 2.96%), ‘network and communication security’ (139 = 10.85%), ‘secure systems design’ (33 = 2.57%), ‘identification and authentication’ (46 = 3.59%) and cryptography (140 = 10.93%).

Of the remaining 45 categories, the most notable include ‘security and privacy’ (28 = 2.18%), ‘copyright and piracy issues’ (17 = 1.32%), ‘security behavior’ (15 = 1.17%), ‘hackers and hacking’ (16 = 1.25%), ‘security polices’ (21 = 1.64%), ‘Public Key Infrastructures’ (17 = 1.32%) and ‘computer forensics’ (29 = 2.26%). This means, therefore, that the remaining 38 categories constitute 216 (16.88%) papers. While the remaining number of 38 additional categories may appear high, an additional category of ‘general IS security’ was introduced (see above), owing to the fact that a number of papers (85) proved difficult to place in the other categories. Hence these papers were assigned to this ‘general’ category.

From another perspective, it is interesting to note the distribution of the 1280 papers in the journals. The three specialized security journals accounted for 1,166 (91.09%) of the papers. Hence the top twenty IS journals contained 114 IS security articles for the period 1990-2004. In fact it should be noted that two of the top twenty IS journals (Database, MISQ Discovery) contained no security papers in this period.

4. Comparing the IS and ISsec Research Practices

4.1 Theories in IS and ISsec research

The importance of the use of theories is widely articulated in IS research (Swanson 1984; Farhoomand, 1987; Benbasat and Zmud, 1999). The discussion of reference theories in IS demonstrates the importance of the use of proper theories. For example, Keen argues that in order for MIS to become a coherent field, there has to be sound reference disciplines from which to build a cumulative research tradition (Keen cited in Culnan, 1986, p. 157). While a number of IS studies have identified reference disciplines (Culnan, 1986, 1987; Barki et. al, 1988, Barki et. al., 1993), a relatively recent study by Vessey et. al. (2002) specifically identified such disciplines based on theories cited in a paper. As part of their research into the diversity of IS, Vessey et. al. (2002) asked the research question ‘What reference disciplines do IS researchers use as the theoretical basis for their publications?’. They report that ‘IS’ emerged as the largest reference discipline (27.2%) followed by ‘Management’ (18.05) and ‘Economics’ (11.0%). Of specific interest to the current paper is the extent to which a theory from a reference discipline was not cited in a paper. Interestingly, the classification category ‘N/A’ described by Vessey et. al. as – ‘A paper either relied on a number of reference disciplines, none of which was dominant, or it did not rely on a reference discipline’ - accounted for only 4.9% of all the papers.

As can be seen, the use of theories in ISsec research is not equally common as it is in IS research. In total only 18.51% of the ISsec articles cited one or more theories. Hence, over 1000 ISsec articles contained no theory whatsoever. As noted, of the 18.51% ISsec papers, nearly 80% cited ‘mathematical’ theory, which leads to the position where the other 37 theories accounted for only 48 ISsec papers. Indeed, thirty of the theories identified were only cited once in the ISsec literature. This indicates that while in ISsec research theories may be cited, intellectual development fails to occur as other researchers do not adopt and explore such theories. Hence these figures generally indicate that IS security research is chronically underdeveloped in terms of theory. This is worrying as with science in general (Laudan, 1984), the use of proper theories are seen as a fundamental element of IS research (Walls et. al., 1992). To summarize, while theories are highly valued in IS, they are not necessary to publish in information security forums.

4.2 Research methods in IS and ISsec

In a relatively early paper, Hamilton and Ives (1982) reviewed the research methods used in the MIS/IS field. Encompassing 532 articles from 15 journals, for the period 1970-1979, they reported how 70% of all the papers were non-empirical in nature. Later studies, however, have witnessed a considerable decrease in this figure. Farhoomand (1987) reviewed a subset of (six) journals analyzed by Hamilton and Ives (1982). Covering the period 1977-1985, 536 articles were assessed. Farhoomand reported 43% were non-empirical in nature compared with Hamilton and Ives' 70%. Such a drop in the number of non-empirical IS papers was mirrored by Farhoomand and Drury's (1999) study. They analyzed eight journals and one conference proceedings (ICIS) for the period 1985 to 1996. In total 2098 papers were assessed, of which, 39% were found to be non-empirical. More recently, Chen and Hirschheim (2004, p. 207) notes that 60 % of IS studies are empirical. The number of empirical studies in the top journal in the field, MISQ, – 72% - in the period 1991 – 2001, illustrates the importance of empirical studies (Chen and Hirschheim 2004, p. 213).

While the preferred research method in IS research is empirical research, an empirical foundation for the research in ISsec is quite weak. In fact, 79% of the ISsec papers were subjective argumentative in terms of their research method. While there is nothing wrong with descriptive and conceptual papers, these results suggest a worrying picture regarding the status of IS security research. While the ISsec field needs to advance intellectually, this is hampered by the lack of empirical research which has taken place. The percentage of ISsec papers in the study which use field experiments (0.07%), surveys (5.31%), case studies (2.65%) and action research (0.07%) illustrate how such intellectual development is hamstrung by the paucity of empirical research into the problems posed in the field. This in itself is problematic, but the lack of empirical research also fails to provide directions for, and a firm basis on which, future research can be based. These problems are compounded further when coupled with the dearth of theory used in the IS security field.

Finally, the low number of theory and empirical research papers in Information Systems Security, Computers & Security and Information Management and Computer Security raise serious doubts about whether these forums can act as target journals for tenure-track faculty.

4.3 Research topics in IS and ISsec

Performing a co-citation analysis based on the MIS literature for the period 1980-1985, Culnan (1987) identified five 'informal clusters of research' including 'foundations', 'psychological approaches to MIS design and use', 'MIS management', organizational approaches to MIS design and use, and 'curriculum'. Culnan concludes her paper by stating:

"The results of this study also provide some counter-intuitive findings regarding the role of technically oriented research and theory within MIS. In this study, no factors are defined by technical research ... While technology and technical issues may have once been central to MIS, the empirical evidence provided by this study suggests that current MIS research has a strong organizational and managerial focus." (pg. 348).

More recent studies have echoed these findings. Taking a different analytical approach, Farhoomand and Drury (1999) used nine categories drawn from the Information Systems Research Library (ISRL) to categorize 2098 IS articles. Eight leading IS journals and the ICIS conference proceedings, for the period 1985-1996, provided the data sources. The nine classification categories included 'reference disciplines', 'external environment', 'technological environment', 'organizational environment', 'IS management', 'IS development and operations', 'IS usage', 'Information Systems' and 'IS education and research'. Farhoomand and Drury's findings revealed that nearly 70% of all the published articles encompassed four research themes, which included 'reference disciplines', 'IS management', 'IS development and operations' and 'information systems'. However, they further noted that 'external environment' 'organizational environment' 'IS education and research' and 'research and reference disciplines' showed 'significantly increasing trends'. This is in contrast to 'IS management', 'IS development and operations' and 'Information Systems' which they argued showed 'significantly decreasing trends'.

Vessey et. al. (2002) in their research on IS diversity used eight major categories ('data/information', 'problem domain', 'computer', 'system software management', 'organizational', 'societal' and 'disciplinary') to classify papers from five leading IS journals for the period 1995-1999. Their analysis found that the topics addressed were predominantly 'organizational' in nature, accounting for 65.6% of all the papers published. This figure was followed by 'problem-domain (11.1%) and 'system software' (7.4%).

Comparing these findings to ISSec, it is perhaps worrying that just 14 topics account for nearly 72% (71.95%) of all the ISsec papers reviewed. IS security is supposedly a broad church covering numerous areas of research and yet relatively few categories account for such a high percentage of the papers. Of the 71.95%, those categories with an overtly technical focus (OS security, viruses and malware, database security, intrusion detection systems, network and communication security, secure systems design, identification and authentication, and cryptography), account for nearly 45% (44.45%) of all the papers. When this analysis is broadened to include other technical topics identified in our analysis (technical certification, digital signatures, wireless security, mobile application security, technical standards, DOS and PC security, firewalls, biometrics, hackers and hacking, Public Key Infrastructures, spam, code security, and computer forensics) the figure rises to 54.45% (697 papers). Hence, only nineteen topics account for this number.

In relation to the above, it has long been recognized that it is important to understand the social as well as technical elements of IS security (Dhillon and Backhouse, 2001). Yet the more 'social' topics in comparison with their technical counterparts have received relatively little attention. For example, our analysis found that just 2 (0.15%) and 7 (0.54%) papers have been written about 'security education' and 'security awareness', respectively. Another category which covers the 'security behavior' of those involved in maintaining security accounted for 15 (1.17%) of all the papers.

5. Explaining the Differences

Having established the key distinctions between IS and ISsec research literature, it becomes clearer that the two areas operate as different fields with different systems of cultural values. Three key distinctions arise: Unlike IS, theory is not a source of symbolic capital in ISsec. Unlike IS, management is not a source of symbolic capital in ISsec. Unlike IS, empirics is not a source of symbolic capital in ISsec.

5.1 Theory is not a strong source of symbolic capital

81.5% of ISsec articles contain no theory. Theory is not a source of symbolic capital in this field. Theoretical thought does not gain admittance to this field. This means that the ISsec habitus does not operate from a history that values theory. Symbolic capital is not derived from a class that thinks about theory. Where theories are present, these are overwhelmingly mathematical (80%), thus the only arena where the habitus might assign symbolic value to theories arises in mathematics.

5.2 Management topics are not a strong source of symbolic capital

48% of ISsec articles are focused on technical issues. Only about a third (35%) have a management focus. The ISsec habitus emphasizes technology over management. Both are a source of symbolic capital, but technology is dominant.

5.3 Empirical methods are not a strong source of symbolic capital

The overwhelming majority of ISsec papers (79%) were subjective argumentation. The ISsec habitus assigns arguments (logic) greater symbolic value than empirics. These arguments are more often based on anecdotes and the reflective practical experience of the authors than scientifically rigorous field research.

The lack of capital derived from either theory or empirical research also suggests that cultural capital in ISsec accumulates outside of academia. This indicates that practical experience is a central source of symbolic capital in this field. As a whole, extensive practical experience in technical areas, together with a logical mind, provides the strongest source of symbolic capital. The long standing history of these values, as indicated by the literature, suggests that this habitus is reproducing these social structures in this field.

6. Discussion and Conclusion

Why does the ISsec research practice place less emphasis on theory and empirical works? One possible explanation is that ISsec research practice has not reached the same maturity level as those found in IS and other scientific

disciplines. This explanation is consistent with the view that an increase in the number of empirical studies indicates increased maturity:

“As a discipline becomes more mature, one might expect theory-testing to outweigh theory-building efforts. Therefore, a comparison between empirical and non-empirical studies serves as a meaningful indication of the progress made in the field. As a field matures, theoretical and conceptual developments become less appealing. Empirical studies, in contrast, become more popular because of the need for theory testing and practical relevance. The growing number of empirical studies might be an indication that the IS field has become more mature and is continuing to evolve.” (Chen and Hirschheim, 2004).

Similar views have been reported in other fields of science and philosophy of science where, from Feyerabend (1964), Popper (1968) and Lakatos (1970) to Thagard (1978) and Laudan (1984), the theory-development and empirical evidence are seen as demarcation criteria that distinguish scientific research from pseudoscience. According to this explanation, ISsec research practice has not matured, and when the field does mature, more empirical research and theory-development follows.

Another possible explanation, in terms of Bourdieu, is that the ISsec research community simply values different forms of social cultural and symbolic capital than does IS research. This explanation means that ISsec is an arena in which traditional academic research, valuing theories and empirical evidence, is not appreciated and will encounter great difficulty in gaining access. This difficulty, like other cultural operations, is reproductive in nature. Without access, no empirical data can be collected. Without empirical data, meaningful research results are limited. Without meaningful research results, the field will continuously assign low value to theory-bound, empirical, management research. With such a low value, no motive for access will be evident. In this way, inaccessibility of the field for theory-bound, empirical, management research is reproduced. The habitus will continue reproduction of the social structures that reserve ISsec research practices for those that are practical, technical, and theory-free.

Can this situation be improved? Changing a culture is not as simple as functionally introducing organizational change. (Indeed, organizational change is problematic.) However, the use of Bourdieu's theories as a basis for explaining the current ISsec research practices does suggest several avenues for introducing change into this field. For example, it is unlikely that the inhabitants of the field can value theory-based, empirical research if it is neither perceived nor understood. Education of security practitioners and researchers may be one important way to enable recognition of the distinctions. Such recognition could dampen the reproduction of the present values. This future education would need to operate at both the masters and doctoral levels worldwide, and should emphasize the value of well-executed, rigorous research. More specifically this education should highlight the importance of empirical research that is based on solid theories.

In a similar manner, well formulated RAE efforts in different countries have the potential to affect the situation (see *EJIS*, vol. 17, no. 2, 2008). If these evaluations reward scholars who publish their works in major (general) IS journals, (those that emphasize theory and empirical evidence), then the reproduction of research practices that do not attend these values will be inhibited. A similar reward structure would be expanded by special issues on IS security in leading IS journals. These will provide an avenue for scholar to publish, in prestigious venues, research that is theory-based and empirical.

A change in the structure of research funding for ISsec research could also play an important role in damping the reproduction of this non-empirical, atheoretical research habitus. Relying extensively on corporate sponsorship for supporting ISsec research amplifies the reproduction of the value system, since the funding sources arise from within the existing habitus. This reproduction could be reduced by introducing more research funding from different quarters – such as government research institutions – that preference basic, rigorous, empirical, and theory-based research.

The habitus of the ISsec research practice is, in key ways, opposite to that of more general IS research practice. The current disciplinary agony of the general IS often regards its lack of relevance to practice and information technology. Perhaps in ISsec we can recognize the results of an opposing agony, a research practice that is just as irrelevant, but in this case because it is too closely embedded in practice and too closely tied to information technology. Future research to better understand how to nudge the ISsec research practices toward better use of theory and empirical data, perhaps through an understanding of the reproduction of its habitus, could help illuminate ways to improve other disciplines, such as the IS discipline itself.

References

- Bacon, C.J. and Fitzgerald, B. (2001). A systemic framework for the field of information systems. *ACM SIGMIS Database*, 32(2), 46-67.
- Bagchi, K. and Udo, G. (2003). An analysis of the growth of computer and Internet security breaches, *Communications of AIS* 12, 684-700.
- Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys* (25) 4, 375-414.
- Baskerville, R. and Wood-Harper, T. (1998). Diversity in information systems action research methods. *European Journal of Information Systems* 7, 90-107.
- Baskerville, R. and Myers, M. (2002). Information Systems as a Reference Discipline. *MIS Quarterly*, 26(1), pp. 1-14.
- Barki, H., Rivard, S. and Talbot, J. (1988). An Information Systems Keyword Classification Scheme. *MIS Quarterly*, 12(2) pp. 299-322.
- Barki, H., Rivard, S. and Talbot, J.A. (1993). Keyword Classification Scheme for IS Research Literature: An Update. *MIS Quarterly*, 17(2) 209-226.
- Benbasat, I., Zmud, R. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly*, 23(1) pp. 3-16.
- Bourdieu, P. (1977). *Outline of a Theory of Practice* (R. Nice, Trans.). Cambridge: Cambridge University Press.
- Bourdieu, P. (1990). *The Logic of Practice* (R. Nice, Trans.). Stanford California: Stanford University Press.
- Bourdieu, P. (1998). *Practical Reason: On The Theory of Action*. Stanford, California: Stanford University Press.
- Burrell, G. and Morgan, G. (1979). *Sociological Paradigms and Organisational Analysis*, Heinemann, London.
- Batts, B and Crawford, L.L. (1991). Problematic progress: A review of Laudan's progress and its problems and science and values. *Journal of the experimental analysis of behaviour*, 55(3), 337-349.
- Chen, W. and Hirschheim, R. (2004) A Paradigmatic and Methodological Examination of Information Systems Research from 1991-2001. *Information Systems Journal*, 14(3), pp. 197-235.
- Culnan, M. (1986). The Intellectual Development of Management Information Systems, 1972-1982: A Co-Citation Analysis. *Management Science*, 32(2), pp. 156-172.
- Culnan, M. (1987). Mapping the Intellectual Structure of MIS, 1980-1985: A Co-Citation Analysis. *MIS Quarterly*, 11(3), pp. 341-353.
- Dhillon, G. and Backhouse, J. (2001). Current directions in information security research: toward socio-organizational perspectives. *Information Systems Journal*, 11(2).
- Farhoomand, A.F. (1987). Scientific Progress of Management Information Systems. *Database*, 18(4), pp. 48-56.
- Farhoomand, A.F. and Drury, D.H. (1999) A historiographical examination of information systems. *Communications of the AIS*, 1, 1-27.
- Feyerabend, P.K. 1964. "Realism and Instrumentalism," in: *The Critical Approach to Science and Philosophy*, M. Bunge (ed.), London: Free Press of Glencoe, 1964, pp. 280-308.
- Culnan, M.J. Mapping the Intellectual Structure of MIS, 1980-1985: A co-citation Analysis. *MIS Quarterly*, 11 (3), 341-354, September 1987.
- Chua, C, Cao, L., Cousins, K and Straub, D. (2002). Measuring Research-Production in Information Systems. *Journal of the AIS* 3, pp. 145-215.
- Galliers, R. (ed.). (1992). *Information systems research: Issues, methods, and practical guidelines*, Blackwell Scientific Publications, Oxford.
- Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, vol30, issue 3, pp. 611-642.
- Hinde, S. (2002). Security surveys spring crop. *Computers & Security*, 21(4), 310-321.
- Hirschheim, R., Klein, H. K., and Lyytinen, K. (1995). *Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations*. Cambridge University Press, UK.
- Hirschheim, R., Klein, H. K., and Lyytinen, K. (1996), Exploring the intellectual structures of information systems development: a social action theoretic analysis, *Accounting, Management and Information Technologies* 6 (1-2), 1-64.
- Iivari, J, Hirschheim, R., and Klein, H. K. (1998). A Paradigmatic Analysis Contrasting Information Systems Development Approaches and Methodologies. *Information Systems Research*, 9(2), 164-193.

- Iivari, J (1991) A paradigmatic analysis of contemporary schools of IS development. *European Journal of Information Systems* 1(4), 249-272.
- Iivari, J. and Hirschheim, R., Klein, H. K. (2001), A Dynamic Framework for Classifying Information Systems Development Methodologies and Approaches. *Journal of Management Information Systems*. Vol. 17(3), 179 – 218.
- Iivari, J, Hirschheim, R., Klein, H.K. (2004). Towards a distinctive body of knowledge for Information Systems experts: coding ISD process knowledge in two IS journals. *Information Systems Journal*, 14, 313–342.
- Kuhn, T.S., 1970. *The Structure of Scientific Revolutions*. (2nd. edition enlarged) Chicago: University of Chicago Press, USA.
- Lakatos, I., Musgrave ed. (1970). *Criticism and the Growth of Knowledge*. Cambridge: Cambridge University Press.
- Landry, M and Banville, C. (1992). A Disciplined Methodological Pluralism for MIS Research. *Accounting, Management and Information Technologies*, 2(2), 77-97.
- Laudan, L., 1984, *Science and Values*. Berkeley: University of California Press, CA, USA.
- Lending, D. and Wetherbe J.C. (1992). Update on MIS Research: A Profile of Leading Journals and U. S. Universities. *Data Base* 23(3), 5-11.
- Peffer, K. and Tang, Y. (2003). Identifying and evaluating the universe of outlets for information systems research: Ranking the journals, *The Journal of Information Technology Theory and Application*, 5(1), 63-84.
- Popper, K. R. *The Logic of Scientific Discovery*, London, Hutchinson, 1968.
- Siponen, M. (2005a). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organization* 15(4), 339–375.
- Siponen, M. (2005b). An analysis of the traditional is security approaches: implications for research and practice. *European Journal of Information Systems*, 14(3), 303–315.
- Siponen, M. and Willison, R. (2007). A Critical Assessment of IS Security Research Between 1990-2004. In Osterle, H., Schelp, J. and Winter, R. (Eds.) *Proceedings of the 15th European Conference on Information Systems (ECIS 2007)*, St. Gallen, June 07-09, 2007, 1551-1559.
- Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly*, 13(2), 147-169.
- Swanson, E.B. "information Systems: Necessary Foundations," presented at the *Conference on the intellectual Foundations for information Professionals*, Emporia State University, Emporia, Kansas, November 15-18, 1984.
- Thompson, D. (1998). Computer crime and security survey. *Information Management & Computer Security*, 6(2), 78–101.
- Thagard, P.R. (1978), Why Astrology Is A Pseudoscience? In *PSA 1978 Volume 1*, edited by P.D. Asquith and I. Hacking (East Lansing: Philosophy of Science Association).
- Truex, D., Holmström, J. and Keil, M. (2006). Theorizing in information systems research: A reflexive analysis of the adaptation of theory in information systems research. *Journal of the AIS*, vol. 7, no. 12, pp. 797-821.
- Vessey, I., Ramesh, V., and Glass, R.L. (2002). Research in Information Systems: An Empirical Study of Diversity in the Discipline and Its Journals. *Journal of Management Information Systems*, 19(2), 129-174.
- Villarroel, R., Fernández-Medina, E. and Piattini, M., (2005). Secure information systems development – a survey and comparison”, *Computers & Security*, 24(4), 308-321.
- Walls, J.G., Wildmeyer, G.R. and El Sawy, O.A. (1992). Building an information systems design theory for vigilant EIS. *Information Systems Research* (3) 1, 36–59.
- Walls, J. G., Widmeyer, G. R., and El Sawy, O. A. (2004). Assessing information system design theory in perspective: How useful was our 1992 initial rendition? *JITTA: Journal of Information Technology Theory and Application*, (6)2, 43-58.
- Walsham, G. (1997). Actor-network theory and IS research: Current status and future prospects. In A. Lee and J. DeGross (eds): *Information Systems and qualitative research*, Chapman and Hall, London, p. 466-480.
- Yin, R.K. (2002). *Case Study Research. Design and Methods*. Third Edition. Applied social research method series Volume 5. Sage Publications. California, 2002.
- Zhang, P and Li, N. (2005). The intellectual development of Human-Computer Interaction Research: A critical Assessment of the MIS literature (1990-2002), *Journal of the AIS*, 6(11), 227-292.